Les activités de Banksys et les nouvelles dispositions en matière de lutte contre la criminalité informatique et de vie privée

Poullet, Yves

Published in:
Aspects juridiques du paiement électronique : actes des colloques Banksys des 25 novembre et 9 décembre 2004

Publication date:
2004

Document Version
le PDF de l'éditeur

Chapitre 4

Les activités de Banksys: ... A l'aune des exigences de la vie privée

Yves Poullet
Doyen de la faculté de droit
Directeur du CRID
FUNDP Namur

L'analyse de l'impact des prescrits de protection des données sur les activités de Banksys oblige à parcourir trois réglementations: la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel soulève quelques questions: celle de la qualification de Banksys dans les opérations qu'elle mène, celle de l'application de quelques principes qui limitent le droit au traitement. Dans ce contexte, la question d'actualité que représente l'éventuelle utilisation de la carte d'identité et de la signature électronique officielle comme carte bancaire.

La deuxième législation abordée n'est encore en Belgique qu'un avant-projet. Il s'agit de la transposition de la directive européenne du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques. Même si l'application de cette directive aux activités de Banksys est discutable, quelques dispositions limitant le droit d'utilisation de certains types de données sont rappelées.

Des réglementations obligent désormais certains détenteurs de données à collaborer avec les autorités judiciaires et policières. Outre la loi de 1993 sur le blanchiment des capitaux, il s'agit de dispositions de procédure pénale inclues dans la loi du 28 novembre 2000 sur la criminalité informatique et l'arrêté royal du 9 janvier 2003 portant exécution de certains articles du Code d'instruction criminelle et de l'article 109*ter* E, § 2 de la loi du 21 mars 1991 portant réforme de certaines entreprises publiques économiques.

1. *Quelques considérations sur les activités de Banksys* – Les activités de l'acteur Banksys se multiplient, s'étendent et se diversifient et nous ne pouvons en ce jour anniversaire que nous en réjouir et féliciter les porteurs de cette initiative économique. Cette constatation n'est pas sans incidence sur la façon dont les lois lui assignent des devoirs nouveaux en matière de protection des données mais également comme «collaborateur» de l'autorité publique afin d'assurer la sécurité publique et de manière plus large la lutte contre la criminalité.

Quelles sont les activités de Banksys? Traditionnellement, Banksys a été le gestionnaire d'un réseau interbancaire belge fournisseur des terminaux d'accès à ce réseau.

Si l'extension géographique des activités du réseau Banksys y compris hors Europe est à signaler, ce qui ne manquera pas à l'avenir de soulever des questions relatives à la légitimité des flux transfrontières de données à caractère personnel, on insiste plutôt sur les nouveaux marchés. Banksys est devenu gestionnaire de réseau pour des émetteurs de cartes de crédit, de cartes shopping, etc. Les terminaux que la société vend, et/ou installe, permettent outre les fonctions traditionnelles de guichets électroniques de paiement, de retraits et autres fonctions bancaires, des paiements à partir de mobiles (paiement WAP) et des transactions via Internet.[1]

1. Sur ces différentes nouvelles applications, lire S. GRIEF, P. WETENHALL et B. MATRE, *Banking in Internet Time*, The Boston Consultancy Group, 2000; T. SCHUDELARO, *Electronic Payment Systems and Money Laundering*, Nijmegen, WLP, 2003. Sur les aspects juridiques des transferts électroniques de fonds par WAP, lire *Les paiements par Wap*, Colloque organisé par le CRID et l'AEDBF les 18 novembre 1999 et 5 octobre 2000, Bruxelles, Bruylant, 2001.

2. *Plan de l'analyse proposée* – Pour analyser l'impact des prescrits de protection des données sur les activités de Banksys, nous nous proposons de parcourir trois législations: la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel soulève quelques questions: celle de la qualification de Banksys dans les opérations qu'elle mène, celle de l'application de quelques principes qui limitent le droit au traitement. Nous aborderons, dans ce contexte, la question d'actualité que représente l'éventuelle utilisation de la carte d'identité et de la signature électronique officielle comme carte bancaire.[2]

La deuxième législation n'est encore qu'un avant-projet.[3] Il s'agit de la transposition de la directive européenne du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques.[4] L'application de cette directive sera discutée et quelques dispositions limitant le droit d'utilisation de certains types de données, rappelées.

Une troisième législation en lien étroit d'ailleurs avec la seconde mérite qu'on s'y arrête. Il s'agit de l'application de dispositions de procédure pénale inclues dans la loi du 28 novembre 2000 sur la criminalité informatique[5] et l'arrêté royal du 9 janvier 2003 portant exécution de certains articles du Code d'instruction criminelle et de l'article 109*ter* E, § 2 de la loi du 21 mars 1991 portant réforme de certaines entreprises publiques économiques.[6]

2. Les cartes d'identité et signatures électroniques officielles ont été introduites dans leur principe par la loi du 25 mars 2003 modifiant la loi du 8 août 1983 sur le registre national (*M.B.*, 28 mars 1983) et ont fait l'objet d'un A.R. du même jour (*M.B.*, 28 mars 2003).
3. Le texte de l'avant-projet de loi actuellement en discussion au Gouvernement a subi des modifications successives. Il a fait l'objet d'un avis de la Commission de protection de la vie privée non encore publié. Pour des raisons évidentes liées au devoir de confidentialité, nous limiterons notre étude à l'analyse du seul texte européen.
4. *J.O.C.E*, L. 201, du 31 juillet 2002, pp. 37-47.
5. A.R. du 9 janvier 2003, *M.B.*, 10 janvier 2003.
6. *Infra*, n° 30.

Section 1

Banksys et la loi du 8 décembre 1992

SOUS-SECTION 1. LES DÉFINITIONS DE BASE

3. *Banksys traite-t-il des données à caractère personnel?* – Que Banksys traite à travers les multiples réseaux qu'elle gère des données à caractère personnel est indéniable. L'identification des clients commerçants, personnes physiques ou lorsqu'il s'agit de personnes morales, des directeurs ou employés en contact avec Banksys est bien évidemment nécessaires à la gestion du contrat portant sur le placement des terminaux et autres services offerts par Banksys. Il va de soi que Banksys identifie directement ses propres clients, ainsi les commerçants ou entreprises ayant installé des terminaux reliés au réseau Banksys pour faciliter les paiements des biens et services qu'ils mettent à disposition.

En matière de cartes bancaires émises à la demande des banques où sont domiciliés les titulaires de compte souhaitant disposer d'une carte, les données de base de la personne concernée, c'est-à-dire des titulaires de carte (nom, prénom, adresse,...) sont nécessaires pour adresser le numéro secret dont l'utilisation conjointe avec la présentation de la carte déclenchera l'opération. Il semble que ces données d'identification directe de la personne concernée sont détruites dès l'émission du numéro secret et l'initialisation de la carte. Peut-on alors considérer que Banksys ne traite plus de données à caractère personnel et parler alors de traitement de données anonymes? Sans doute, les données conservées par Banksys au-delà de cette période n'identifient plus directement la personne concernée: le titulaire du compte bancaire qui active grâce à sa carte le paiement ou le titulaire de la carte de fidélité. Cependant, il est clair que les numéros d'une telle carte ou du compte bancaire liés à la carte rendent indirectement possible l'identification concrète de la personne concernée, dans la mesure où Banksys pourrait interroger la banque auprès de laquelle le compte est ouvert ou l'entreprise qui délivre la carte de fidélité afin de connaître l'identité de la personne concernée. Bref, la donnée détenue par Banksys rend la personne titulaire de la carte identifiable par recours à un tiers. On note que le fait que Banksys s'engagerait à ne pas rechercher l'identité des personnes titulaires de carte ne changerait rien à nos conclusions. C'est la possibilité *in abstracto* d'identifier la personne physique et non la réalisation de cette possibilité ou la vraisemblance de cette réalisation qui rende la loi applicable.[7]

A cet égard, le considérant 26 de la directive est particulièrement clair: «Considérant que les principes de la protection doivent s'appliquer à toute information concernant une personne physique identifiée ou identifiable; que pour déterminer si une personne est identifiable, il convient de considérer l'ensemble des moyens susceptibles d'être raisonnablement mis en œuvre, soit par le responsable du traitement, soit par une autre personne, pour identifier ladite personne;...». L'exposé des motifs de la loi du 8 décembre 1992 (*Doc. parl.*, Ch. repr., sess. ord. 1997-1998, n° 1566/1, p. 12) se réfère explicitement à ce considérant nonobstant l'avis de la Commission plus nuancée. Sur cette controverse et notre critique de la solution belge jugée trop stricte, Th. LÉONARD-Y. POULLET, 'La protection des données à caractère personnel en pleine (r)évolution', *J.T.*, 1999, p. 378, n° 3 *in fine*.

4. *Banksys: un sous-traitant ou un responsable?* – Si les données traitées par Banksys sont indiscutablement des données à caractère personnel, Banksys est-il pour autant responsable des traitements qu'il opère ou n'est-il que sous-traitant d'opérations effectuées pour compte de tiers. Les définitions de la loi sont les suivantes. L'article 1er, § 4 de la loi définit comme suit, le responsable du traitement: *«la personne physique ou morale, l'association de fait ou l'administration publique qui seule ou conjointement avec d'autres, détermine les finalités et les moyens du traitement de données à caractère personnel»*; le § 5 du même article énonce, quant à lui, la définition du sous-traitant: *«la personne physique ou morale, l'association de fait ou l'administration publique qui traite des données à caractère personnel pour le compte du responsable du traitement et est autre que la personne qui, placée sous l'autorité directe du responsable, est habilitée à traiter les données»*.

Banksys opère-t-il certains traitements pour son compte ou l'ensemble des traitements opérés correspondent-ils uniquement à des missions effectuées pour compte de tiers, c'est-à-dire pour les banques, le cas échéant, pour les entreprises? La réponse à cette alternative a des implications dans la mesure où la qualification de Banksys comme responsable de traitements entraîne pour elle certaines obligations administratives (déclaration des traitements auprès de la Commission de protection de la vie privée, obligation d'information des personnes concernées, etc.) alors que la seconde branche de l'alternative qui voit Banksys comme un sous-traitant oblige les responsables qui font appel à ce sous-traitant de conclure par écrit un contrat qui, notamment, précise les missions et fixe la responsabilité du sous-traitant.[8]

5. *Une réponse difficile* – Sans doute, peut-on considérer dans une première approche que l'émission des cartes et codes secrets, les mesures de sécurité prises par Banksys, y compris la gestion de black lists[9], la présentation en compensation des différents ordres de paiement, l'établissement pour les cartes de fidélité de compte client sont des missions que Banksys opère pour des tiers: les banques, d'une part; les entreprises émettrices de cartes de fidélité, d'autre part.

On peut, au contraire, deuxième option, considérer que l'ensemble de ces traitements est opéré par Banksys de manière autonome et constitue le service propre de réseau sécurisé que Banksys offre à ses clients sans possibilité pour ceux-ci de les moduler et de les adapter à leurs besoins propres.

8. D'autres exigences sont reprises à l'article 16, § 1er, ainsi, le choix d'un sous-traitant offrant des garanties adéquates en matière de sécurité.
9. A cet égard, il semble que la tenue des black lists ne soit plus centralisée par Banksys mais décentralisée auprès de chaque banque et les oppositions soient dès lors directement générées par les banques, participantes au réseau Banksys. Cette situation, si elle se confirme, représente un progrès considérable dans la mesure où elle évite les risques d' une liste centralisée.

On pourrait, enfin, troisième option, estimer que Banksys définit conjointement avec les banques les finalités et les moyens du traitement. En effet, la structure du réseau, son mode de fonctionnement, les services à rendre par Banksys aux membres de ce réseau sont décidés de commun accord entre Banksys et ces derniers.[10] Il s'agit bien alors de considérer que Banksys est responsable des traitements opérés au sein du réseau, en même temps que les banques qui participent à ce réseau. Ce qui implique notamment qu'une personne concernée qui verrait sa vie privée violée par exemple pour défaut de sécurité du réseau Banksys pourrait se retourner sur les deux responsables conjoints.

Le propos serait peut-être à nuancer pour certains services particuliers de réseau que des entreprises négocieraient auprès de Banksys dans le cadre de l'émission de cartes de fidélité. Dans de tels cas, c'est souvent l'entreprise qui fixe les missions particulières de Banksys et définit les finalités et les moyens des traitements que Banksys se doit d'opérer. Banksys est alors sous-traitant et s'appliquerait alors l'article 16, § 1er, de la loi de 1992.

Tel n'apparaît pas le cas vis-à-vis de traitements opérés dans le cadre du réseau de paiement interbancaire. La nature et les caractéristiques des traitements offerts par Banksys sont sans doute discutées avec les banques et, le cas échéant, adaptées à leurs besoins mais répondent à des finalités propres à Banksys, en tant qu'opérateur de réseau qui offre à la communauté bancaire des services à valeur ajoutée du fait de leur commune participation au réseau.

Banksys apparaît bien alors comme responsable du traitement même si c'est conjointement avec les banques qu'il détermine les «finalités» et les «moyens du traitement» de données à caractère personnel.

SOUS-SECTION 2. LES OBLIGATIONS DE BANKSYS

6. *Préambule* – La qualité de responsable du traitement entraîne pour Banksys certaines obligations administratives, telles la déclaration à la Commission (art. 17 de la loi), mais au-delà et, de façon plus essentielle, des obligations de sécurité (art. 16 de la loi), celles de veiller à la légitimité des traitements (art. 4 à 9 de la loi) et au respect des droits de la personne concernée (art. 10 à 15*bis* de la loi).

Notre propos sera bref tant en ce qui concerne l'obligation de sécurité que celle du respect des droits de la personne concernée. Nous nous attarderons plus longuement sur la question de la légitimité des traitements.

10. Le même raisonnement s'applique à notre avis à propos de différentes coopératives créées à l'intérieur de secteur (Préventel pour le secteur de la mobilophonie; Datassur, pour le secteur des assurances;...). Dans tous ces cas, on peut, me semble-t-il, considérer que la définition des moyens et des finalités des traitements est fixée conjointement par les entreprises du secteur et la société ou coopérative créées pour la gestion des traitements communs. Dans le même sens, D. DE BOT, *Verwerking van persoonsgegevens*, Kluwer, Recht en Praktijk, n° 30, p. 50, n° 63 *in fine*.

7. *La sécurité du réseau: une obligation* – L'obligation de sécurité prévue par l'article 16 de la loi vise non seulement à assurer la confidentialité mais également l'intégrité des données.[11] Cette double facette de l'obligation de sécurité doit être assurée tant par des moyens techniques qu'organisationnels conformes aux exigences des règles de l'art correspondant à la nature des données traitées et aux risques liés aux caractéristiques du traitement.[12]

Ainsi, Banksys soumettra à des obligations contractuelles de confidentialité les membres du personnel opérateurs réseaux, désignera les employés en charge de contrôler la mise à jour des listes noires, etc. Ainsi, Banksys utilisera des techniques adéquates de cryptage pour la transmission de données, en particulier lorsqu'il emprunte les réseaux publics RNIS, PSTN, ADSL ou mobilophonique, avant d'atteindre son réseau propre BankNET, il veillera, le cas échéant, à la mise à jour des listes d'opposition des cartes perdues et volées et adaptera le niveau de sécurité des moyens d'authentification et de signature afin d'éviter la falsification de ceux-ci.[13]

8. *Banksys et les droits des personnes concernées* – Le droit des personnes concernées à l'information quant à l'existence des traitements de Banksys, le responsable du traitement et les finalités de celui-ci, est prévu par l'article 9 de la loi. Il s'exercera naturellement par les entreprises auxquelles les personnes concernées sont liées.[14]

Ainsi, l'émetteur de la carte de fidélité «carburant» se doit de mentionner que les demandes de paiement effectuées grâce à la carte sont autorisées et transmises y compris quelques données supplémentaires via Banksys. L'information donnée précisera qu'outre cette transmission, Banksys effectue les démarches permettant le débit du compte du titulaire de la carte (celui-ci ne se confond pas nécessairement avec l'utilisateur) et le crédit du compte du commerçant (le pompiste).

A propos du droit d'accès consacré par l'article 10 de la loi, la demande pourra être opérée directement auprès de Banksys si celui-ci est jugé responsable du traitement (*cf. supra* n° 5). Il s'agirait par exemple pour le client d'une banque contestant certaines utilisations de sa carte de banque à partir de guichets automatiques d'obtenir de Banksys les traces de tel ou tel retrait.

9. *Une question délicate: les systèmes automatisés de décision* – La légitimité des systèmes automatisés de décision est abordée par l'article 12*bis* de la loi qui stipule: «Une décision produisant des effets juridiques à l'égard d'une personne

11. ... ce qui peut être important. Ainsi, une erreur de transmission ou le blocage du système Banksys peuvent provoquer des imputations incorrectes dans les comptes d'un client d'une banque et avoir des conséquences dommageables: refus d'une prestation, charges d'intérêts.
12. Le fait que le réseau Banksys couvre la quasi-totalité des opérations électroniques de paiement et fournit des services essentiels à la population plaidera pour l'adoption de mesures de sécurité importantes.
13. A cet égard, les dangers liés avec la reproduction du numéro de la carte sur le ticket souche remis, à l'issue d'une opération de paiement, à son émetteur.
14. Il est à noter que rien n'est prévu par la loi sur les modalités de l'information. L'information est due mais peu importe par quel media.

ou l'affectant de manière significative ne peut être prise sur le seul fondement d'un traitement automatisé de données destiné à évaluer certains aspects de sa personnalité». On relève que le fonctionnement d'un réseau comme Banksys repose bien évidemment – sécurité oblige – sur ce type de logiciel d'aide à la décision, ainsi le système automatisé d'autorisation par reconnaissance du moyen d'authentification pouvant mener au blocage de la carte ou le système de vérification automatique des limites d'autorisation à propos d'un type d'opération particulière.

On peut facilement imaginer les conséquences d'une telle décision automatisée: l'interdit de carte dans un monde où l'accès au guichet physique d'une banque peut être difficile (période de congé, regroupement des succursales) et où cet accès à un moyen de paiement doit être obtenu dans l'urgence (l'automobiliste en panne d'essence à une heure du matin devant une pompe «tout automatique»).

L'alinéa 2 de l'interdiction admet que, par contrat, la personne concernée puisse accepter de tels systèmes automatisés d'aide à la décision. Sans doute, les contrats de remise des cartes électroniques devraient prévoir une telle disposition et la porter raisonnablement à la connaissance des porteurs de carte. L'alinéa 2 ajoute que le contrat «doit» contenir des mesures appropriées garantissant la sauvegarde des intérêts légitimes de l'intéressé, en particulier lui permettre utilement de faire valoir son point de vue. L'existence d'une hot line permettant de prévenir Banksys ou son représentant (la Banque ou l'entreprise avec lesquelles la personne concernée est en relation) apparaît nécessaire au vu d'une telle disposition.

SOUS-SECTION 3. LA LÉGITIMITÉ DES TRAITEMENTS DE BANKSYS

10. *Préambule* – Les données traitées par Banksys sont, comme nous le verrons (*infra*, n° 17) essentiellement des données de trafic et de localisation. La légitimité du traitement de telles données est précisée, au-delà des prescrits de la directive générale en matière de vie privée, par les dispositions de la directive 2002/58 déjà citée dont nous étudierons à la Section 3, la portée.

Notre propos ici est double: comme l'introduction le précisait, Banksys diversifie ses services. Sans doute, est-il bon de rappeler le principe de leur étanchéité!

Secondement, l'idée développée par certains est de coupler la carte d'identité électronique et celle dite de banque dans la mesure où le système et les moyens d'authentification et de signature présents ou susceptibles d'être présents sur la carte d'identité officielle pourraient également être utilisés par les services Banksys et lisibles par les terminaux Banksys. Cette possibilité nous permettra d'évoquer la question des cartes multifonctionnelles.

11. *L'étanchéité des traitements* – L'article 4, § 1er, 2° de la loi du 8 décembre 1992 tel que modifié par la loi du 11 décembre 1998 énonce: *«Les données doivent être collectées pour des finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement de manière incompatible avec ces finalités, compte tenu de*

tous les facteurs pertinents, notamment des précisions raisonnables de l'intéressé et des dispositions légales et réglementaires applicables».

Cette disposition peut recevoir dans le cas des services offerts par Banksys de nombreuses applications. Ainsi, on pourrait imaginer que le croisement des données générées par les différentes cartes d'un même porteur soit effectué par Banksys et puisse servir à un meilleur profilage d'un consommateur. Si une telle possibilité apparaît dans l'état actuel irréaliste dans la mesure où Banksys ne conserve pas les données d' identification des porteurs de carte[15], ces croisements opérés à partir de traitements ayant chacun leurs propres finalités: la gestion des opérations de paiement liées à l'utilisation de telle ou telle carte, excèdent les prévisions raisonnables des personnes concernées et sont donc «incompatibles» aux yeux de la loi vie privée.

De même, on pourrait imaginer que Banksys développe pour une entreprise, des logiciels permettant de définir la productivité des employés aux caisses des grands magasins à partir du nombre de paiements électroniques y effectués. Sans doute, Banksys n'agit-elle là que comme sous-traitant mais il est clair que ce traitement relatif aux employés est incompatible avec la finalité de la collecte à savoir assurer les paiements électroniques générés par les cartes des clients.

12. *Belpic ou le couplage des cartes bancaires et d'identité* – On pourrait de même imaginer le couplage des cartes bancaires, de crédit voire de fidélité avec la carte d'identité et l'utilisation de la signature officielle comme modes d'authentification et de signature liés à l'utilisation de telles cartes.

Ce couplage dont l'intérêt pour les administrations et les entreprises est évident[16] soulève du point de vue de la loi vie privée quelques problèmes. La lecture par les terminaux multifonctionnels[17] de la carte d'identité et de son contenu pourrait permettre à Banksys d'avoir accès et de traiter des données présentes

Elle ne serait possible qu'à propos du croisement des données générées par l'utilisation des cartes de crédit et de paiement bancaire dans la mesure où ces données se réfèreraient à un compte bancaire identique.

Ainsi, le fait qu'un seul lecteur et l'introduction d'une seule carte permettent à la fois la transaction avec l'administration et son paiement, facilite la vie des administrations publiques. Du côté des entreprises, on se réjouira de voir se multiplier l'utilisation d'une signature électronique «sûre», officielle et quasiment gratuite. Pour le citoyen, on soulignera le fait qu'une seule carte suffit et qu'un seul mot de passe ouvre aussi bien les portes des administrations que des commerçants.

Sur la question délicate des cartes à puce multifinctionnelles, le lecteur se référera à l'article publié par E. KEULEERS et J.M. DINANT, 'Multi-application smart card schemes', 19 *CLSR*, 4, 2003, pp. 480 et s.; 20 *CL&SR*, 1, 2004, pp. 22 et s.; 20 CL&SR, 3, à paraître. Cet article s'appuie sur les réflexions menées par les auteurs dans le cadre du développement d'un projet de cartes multifonctionnelles mené à Southampton (UK) par diverses administrations, l'université et quelques opérateurs semi-publics. Il suggère des développements technologiques aptes à répondre aux exigences des législations vie privée.

sur la carte, ainsi la photo digitalisée, le numéro de registre national. Sans doute, faudra-t-il, comme le réclame la Commission de protection de la vie privée[18], veiller à ce que de telles informations présentes sur la carte d'identité ne soient accessibles que par les seules administrations autorisées de la carte d'identité.[19]

13. *Belpic et la sécurité* – Un second point mérite d'être relevé: le projet Belpic ne semble pas distinguer le PIN code d'authentification, de celui de la signature.

Cette confusion crée un manque de sécurité: il va de soi que la multiplication des utilisations de la carte d'identité comme mode d'authentification risque d'entraîner le porteur de la carte à divulguer à ces proches son PIN code et donc à générer des risques de falsification de sa signature électronique. L'article 16 de la loi vie privée rappelle au responsable des traitements son obligation de sécurité. Sans doute, serait-il utile à cet égard que comme d'autres pays, chacune des deux fonctions soit associée à un PIN code particulier! Par ailleurs, chaque vérification du certificat auquel sont liés le mode d'authentification et la signature engendre normalement auprès du certificateur (en l'occurrence, le prestataire de certification choisi par le Gouvernement: Belgacom) une donnée attestant de l'utilisation de ces dernières, ce qui lui permet de connaître l'existence de toutes les opérations générées qu'elles concernent une transaction avec l'administration ou un paiement privé.[20]

18. *Cf.* à cet égard, l'avis n° 19/2002 de la CPVP du 10 juin 2002 relatif au projet de loi modifiant la loi du 8 août 1983 organisant un registre national.
19. L'article 16 de la loi du 8 décembre 1992 oblige le responsable du traitement à mettre en place des mesures techniques (hardware et software) de sécurité de manière à prévenir des transmissions ou accès non autorisés. On citera aussi l' opinion du groupe 29 (opinion 7/2000 du 2 novembre 2000) qui prescrit que le design des technologies de traitement de l'information tant sur le plan du matériel que du logiciel doit être conforme aux finalités du traitement, restreindre les données aux seules nécessaires et faciliter l'exercice par la personne concernée de ses droits.
20. Les auteurs de l'article sur les cartes multifonctionnelles citées *supra* note 16 suggèrent de dissocier le Global Unique Identifier lié à la carte, des clés d'authentification et de cryptographie particulières par type d'applications ce qui recréerait une certaine étanchéité entre les différents types d'application présents sur la carte et liés à des responsables de traitement distincts.

Section 2

Banksys et la directive dite «vie privée et communications électroniques»

14. *Présentation de la directive* – La directive 2002/58 du 12 juillet 2002 sur le point d'être transposée dans notre pays[21] est une directive sectorielle applicable selon l'article 3 aux «fournisseurs de services de communications électroniques au public sur les réseaux publics de communications électroniques». Elle entend dans le cadre de ce champ d'application particulier, non point déroger à la directive générale mais préciser quelques limites et obligations supplémentaires, liées aux risques accrus que représente, pour la protection des données personnelles, l'utilisation des technologies de communication sans frontières et dotées de capacités de traitement accrues.[22]

L'application de cette directive aux activités de Banksys est discutable même si nous la croyons justifiée.[23] Si la directive est applicable, certaines de ses obligations méritent l'attention de Banksys.

SOUS-SECTION 1. LA DIRECTIVE 2002/58/CE EST-ELLE APPLICABLE AUX ACTIVITÉS DE BANKSYS?

15. *Champ d'application de la directive* – Les notions qui permettent de circonscrire le champ d'application fixé par l'article 3 de la directive, rappelé ci-dessus, supposent que soient définies les notions de «services de communications électroniques offerts au public» et de «réseaux publics de communications électroniques». On notera que la directive ne se réfère pas à la notion de «responsable du traitement» pour fixer les obligations contenues dans la directive. En d'autres termes, la directive 2002/58/CE est applicable à un fournisseur de services de communications électroniques offerts au public sur des réseaux publics de communications électroniques quand bien même celui-ci ne pourrait pas être qualifié au sens de la directive 95/46/CE de responsable du traitement mais de simple sous-traitant.

Par «services de communications électroniques» il faut entendre «le service fourni normalement contre rémunération qui consiste entièrement ou principalement en la transmission de signaux sur des réseaux de communications électroniques».[24] Plusieurs caractéristiques sont à souligner: il s'agit d'un service principalement de transmission et non de contenu, souligne le considérant 5 de la directive. Il s'agit donc d'un service consistant en l'envoi de contenus, «c'est-à-dire l'exploitation d'un réseau et la transmission même des contenants sur ce réseau», en l'occurrence la transmission des instructions de paiement ou d'opérations déclenchées à partir de cartes de paiement ou de fidélité. L'exigence de la rémunération ne pose pas de difficulté dans la mesure où le paiement du service ne doit pas nécessairement provenir de l'émetteur de l'instruction, le bénéficiaire premier du service, mais peut consister en une subvention par une entité tierce[25], les banques ou les entreprises, distributrices des cartes de fidélité.

La seconde notion pose par contre difficulté: le service doit être accessible au public «sur les réseaux publics de communications électroniques». La notion est définie par l'article 1/a) de la directive 2002/21/CE relative aux services de communications électroniques[26] comme des réseaux utilisés entièrement ou principalement pour la fourniture de services de communication accessibles au public. En d'autres termes, la directive 2002/58/CE ne serait pas applicable aux réseaux dits «fermés». Que dire à propos de Banksys, certes le réseau est principalement un réseau propriétaire mais la plupart des services qu'il offre est accessible au public, c'est-à-dire aux «participants d'un marché relevant», comme les clients d'un compte bancaire.[27]

On relèvera que la frontière entre un service accessible au public en général et un service réservé n'est pas aisée. Ainsi, certaines cartes dites entreprises comme celles émises par les entreprises pétrolières, sont réservées aux membres des sociétés ayant acquis le droit d'utiliser ces cartes. Faut-il exclure ces services de l'application de la directive? Sans doute, même si le Groupe de l'article 29 conteste la distinction opérée par la directive, en soulignant que les risques d'atteinte à la protection des données liées au développement de réseaux fermés, comme les intranets sont évidents et méritent la même protection que celle prévue par la directive.[28]

21. A cet égard, le texte d'un avant-projet de loi déjà soumis à l'avis de la Commission de protection de la vie privée a été récemment soumis au Conseil des ministres pour la seconde fois. On note que cet avant-projet transpose le «paquet» des cinq directives destinées à réformer.
22. A cet égard, les considérants n^{os} 5 et 6 de la directive 2002/58/CE.
23. Pour un exposé complet sur la directive, lire J. DHONT et K. ROSIER, «Directive vie privée et communications électroniques: premiers commentaires», *Rev. Ubiquité-Dr. Tech. Info*, 2003/15, pp. 7-46; S. LOUVEAUX et V. PEREZ ASINARI, «New European Directive 2002/58 on the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector – Some Initial Throughts», *Computers and Telecommunications Rev.*, 2003, n° 5, pp. 133-138.
24. Cette définition est donnée par l'article 2 c) de la directive 2002/21/CE, J.O. L 108, 24 avril 2002, pp. 33-50.
25. *Cf.* l'avis n° 7 du groupe 29, concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques, p. 5 disponible à: *http://europa.eu.int/comm/internal_market/en/dataprot/wpdocs/wp36.p.pdf*
26. J.O.L. 108, 24 avril 2002, pp. 33-50 (voir également l'article 2(b) de la directive 2002/22/CE publié le même jour au J.O., pp. 51-70).
27. A cet égard, voir la Commission en date du 20 octobre 1995 de la Commission au Parlement européen et au Conseil sur le statut et la transposition de la directive 90/388/CE sur la concurrence dans le marché des services de télécommunications, 95/C 275/02, J.O. C275, p. 2: La notion de «pour le public» n'est pas définie dans la directive et doit être comprise dans le sens commun: un service «pour le public» est un service disponible pour le public sur une base égale. Un groupe fermé est un groupe d'entités ou d'individus, non nécessairement lié par des liens économiques mais qui peuvent être identifiés comme membre d'un groupe sur base d'une relation professionnelle entre eux, ou avec une autre entité du groupe pour lequel le besoin de communication interne résulte d'un intérêt commun à la base de cette relation.
28. Opinion 7/2000 émise par le Groupe dit de l'article 29 à propos de la proposition de la Commission européenne pour l'adoption de la directive du Parlement européen et du Conseil relative au traitement des données à caractère personnel dans le secteur des communications électroniques, disponible sur le site: http://.

SOUS-SECTION 2. QUELQUES CONSÉQUENCES DE L'APPLICATION DE LA DIRECTIVE

§ 1. Le champ d'application de la directive

16. *La protection des personnes morales* – On sait que l'article 1er, dans son deuxième paragraphe, prévoit la protection par la directive des abonnés qui sont des personnes morales. Cette disposition est remarquable dans la mesure où la directive 95/46 ne vise que la protection des personnes physiques. Le considérant 12 de la directive 2002/58/CE mentionne ainsi le devoir de protéger les intérêts légitimes des «personnes morales», sans définir plus avant cette notion.

Que Banksys traite des données relatives à des personnes morales est une évidence, tantôt, il s'agit de clients directs de Banksys, ainsi les terminaux de paiement installés dans une entreprise peuvent révéler indirectement le chiffre d'affaires de cette entreprise; tantôt, il s'agit de clients de Banksys, ainsi lorsqu'une compagnie pétrolière délivre des cartes à des entreprises, il obtient par ce biais des renseignements à la fois sur l'activité de cette entreprise et sur l'activité des membres de son réseau de distribution. Le contenu de toutes ces données équivaut bien à un intérêt légitime de ces entreprises dans la mesure où la révélation d'un chiffre d'affaires à un tiers non autorisé peut avoir des conséquences graves sur l'entreprise. Il est clair que la protection de ces intérêts légitimes de toutes personnes morales passe par certains devoirs de confidentialité (art. 5) et de sécurité du réseau (art. 6) et que les dispositions relatives aux données de trafic et de localisation que nous aborderons ensuite s'appliquent à ce type de données.

17. *La distinction abonnés-usagers* – La distribution par une entreprise de cartes aux membres de son personnel (par exemple, les cartes de crédit entreprises; les cartes carburant distribuées par une entreprise de transport aux différents conducteurs) soulève une autre question: celle de la distinction entre «l'abonné» à un service qui peut être une personne morale et «l'utilisateur» qui est la «personne physique» utilisant un service de communications électroniques accessibles au public à des fins privées ou professionnelles sans être nécessairement abonnée à ce service.

Cette distinction existe également lorsqu'il faut émettre différentes cartes de crédit pour les membres de sa famille.

Il est clair que la réception par l'abonné[29] de données relatives aux utilisateurs permettra aux premiers d'obtenir certains renseignements sur les seconds et de contrôler, ainsi, les activités professionnelles ou privées de ces derniers. La directive prévoit certaines obligations à charge du fournisseur d'un service de communication électronique, directement en faveur des utilisateurs; ainsi, l'obligation d'informer les utilisateurs de la possibilité via le réseau de stocker des informations ou d'accèder à des informations stockées sur le terminal de l'utilisateur; ainsi, l'obligation de donner à l'utilisateur les informations quant aux types de données de trafic et de localisation traitées, etc.

29. Peut-on à propos des membres du réseau comme les banques parler «d'abonnés», la question n'est pas simple à résoudre.

Sans doute, Banksys s'acquittera aisément de ce devoir par document informatif attaché directement à la carte dont la remise accompagnera la délivrance de la carte de crédit, de paiement ou de fidélité.

§ 2. Les données traitées

18. *Les données de localisation et de trafic* – Les articles 6 et 9 définissent un régime particulier dérogatoire aux principes généraux de la directive 95/46 pour les données dites de localisation et de trafic. Ces données sont définies comme suit par l'article 2 de la directive.

«b) données relatives au trafic: toutes les données traitées en vue de l'acheminement d'une communication électronique ou de sa facturation;

c) données de localisation: toutes les données traitées dans un réseau de communications électroniques indiquant la position géographique de l'équipement terminal d'un utilisateur d'un service de communications électroniques accessible au public;»

Quelques données acheminées via le réseau de Banksys constituent des données de trafic et de localisation. Ainsi la donnée sur l'émetteur du message identifié par un numéro de carte et sur le destinataire, l'émetteur de la carte, le lieu et le moment précis de la transaction constituent des données de trafic. La donnée relative au contenu du message, le montant de la transaction échappe à ces deux catégories de données.

Les dispositions de la directive (art. 6 et 9) contiennent diverses limites à la collecte et l'utilisation de telles informations:

- les utilisateurs et abonnés doivent être informés des types de données traitées et de la durée de traitement;
- le traitement de telles données doit être restreint aux personnes agissant sous l'autorité des fournisseurs de réseaux publics de communication et de services de communications électroniques accessibles au public qui sont chargés d'assurer la facturation ou la gestion du trafic, de répondre aux demandes de la clientèle, de détecter les fraudes et de commercialiser les services de communications électroniques ou de fournir un service à valeur ajoutée; ce traitement doit se limiter à ce qui est nécessaire à de telles activités;
- les données doivent être effacées ou rendues anonymes dès qu'elles ne sont plus nécessaires à la transmission sous trois réserves.

19. *Quelques réflexions à propos des réserves* – Les articles 6 et 9 mentionnent diverses exceptions permettant de traiter les deux types de données en question de manière plus étendue. L'une sera traitée ultérieurement. Elle vise l'obligation de rétention des données de trafic ou de localisation que la loi peut imposer à des fins d'investigation et de poursuites d'activités criminelles. Les deux autres réserves consistent la première à permettre l'allongement de la durée de traitement pour des fins de facturation des abonnés. «*Un tel traitement n'est autorisé, dit*

l'article 6.2 que jusqu'à la fin de la période au cours de laquelle la facture peut être légalement contestée ou des poursuites engagées pour en obtenir le paiement». L'application de cet article justifiera la conservation par Banksys des données de trafic et de localisation pendant toute la durée où des contestations sur la réalité d'une transaction peuvent être produites tant par les banques ou entreprises, clientes de Banksys que par les utilisateurs du service.

Sans doute, ce délai devrait être fixé et une information claire sur ce délai être fournie tant aux abonnés qu'aux utilisateurs.

La seconde réserve concerne les services à valeur ajoutée susceptibles d'être offerts par le fournisseur de services. Ainsi, on peut songer que Banksys offre à des entreprises qui utilisent son réseau et ses terminaux des services à valeur ajoutée comme un récapitulatif par carte, un tableau comparatif par carte au terminal, etc.

De tels services supplémentaires peuvent justifier la conservation des données au-delà des besoins de facturation ou de contestation, par exemple si le comparatif est opéré sur plusieurs années on intègre des données rendues anonymes relatives à d'autres abonnés. On notera que dans ce cas, outre l'information à donner tant à l'abonné qu'à l'utilisateur, leurs consentements doivent être obtenus et peuvent être révoqués à tout moment.

§ 3. La sécurité et les terminaux

20. *Un devoir particulier de sécurité* – L'article 4 de la directive adapte aux particularités d'un service de transmission électronique par réseau, les exigences de l'article 16 de la directive générale 95/46/CE.

Nous en reprenons ici le texte particulièrement clair: «*1. Le fournisseur d'un service de communications électroniques accessible au public prend les mesures d'ordre technique et organisationnel appropriées afin de garantir la sécurité de ses services, le cas échéant conjointement avec le fournisseur du réseau public de communications en ce qui concerne la sécurité du réseau. Compte tenu des possibilités techniques les plus récentes et du coût de leur mise en œuvre, ces mesures garantissent un degré de sécurité adapté au risque existant.*

2. Lorsqu'il existe un risque particulier de violation de la sécurité du réseau, le fournisseur d'un service de communications électroniques accessible au public informe les abonnés de ce risque et, si les mesures que peut prendre le fournisseur du service ne permettent pas de l'écarter, de tout moyen éventuel d'y remédier, y compris en indiquant le coût probable.»

L'article 5 traite du devoir du fournisseur d'assurer la confidentialité du contenu des messages, des données de trafic et de localisation et de prévenir de ce fait toute interception des données ainsi transmises. Toute atteinte à la confidentialité présumera, selon l'article 23 de la directive transcrit par l'article 15*bis* de la loi belge une faute du fournisseur et entraînera la responsabilité de celui-ci sauf à

lui de démontrer que le fait qui a provoqué ce dommage ne lui est pas imputable.[30]

21. *Implications particulières de l'article 5.3.* – Le point 3 de l'article 5 déjà cité est particulièrement important: le fournisseur du service est tenu d'informer l'utilisateur du service du fait qu'il stocke des données sur le terminal de ce dernier ou accède à des données. Il doit permettre à l'utilisateur de refuser un tel traitement.

L'introduction d'une carte dans un lecteur permet au réseau d'y lire ou d'y inscrire des données. Lors de notre discussion à propos du couplage de la carte d'identité et des cartes de paiement nous posions déjà la question de la légitimité de terminaux de paiement permettant de lire toutes ou certaines données inscrites sur la carte d'identité. On peut parfaitement de même imaginer que la carte soit utilisée comme support pour l'inscription de données tels le nombre d'essais infructueux d'introduction d'un code PIN, l'existence de certains privilèges du titulaire voire l'instruction donnée par la carte de transférer les données à telle entreprise connectée au réseau.

Dans la mesure où la carte doit être considérée comme un équipement terminal au sens de la directive[31], l'article 5.3. exige le consentement de la personne concernée, ainsi qu'une possibilité pour l'utilisateur de désactivation au cas par cas de la réception ou de l'émission de messages par le terminal.

A propos de la configuration «privacy compliant» des équipements terminaux qu'il s'agisse des cartes ou des lecteurs de cartes, la disposition de l'article 14.3 qui permet à la Commission «au besoin», d'adopter des mesures «*afin de garantir que les équipements terminaux soient construits de manière compatible avec le droit des utilisateurs de protéger et de contrôler l'utilisation de leurs données à caractère personnel*».

Cette disposition traduit l'obligation des fournisseurs d'équipements terminaux de veiller à ce que leurs équipements ne puissent permettre des traitements non autorisés. Ainsi, Banksys veillera à ce que les entreprises ne puissent coupler leurs propres équipements (par exemple, la caisse d'un grand magasin) aux lecteurs de cartes installés par Banksys afin d'y lire et de copier certains éléments comme le numéro de la carte de paiement utilisée.[32] Une telle transmission outre qu'elle peut apparaître déloyale vu son caractère peu transparent serait contraire à la loi de 1992 dans la mesure où la transmission de cette donnée n'est pas

30. Sur ce renversement de la charge de la preuve, lire Y. POULLET, J-F. LEROUGE, 'La responsabilité des acteurs de l'Internet', in *Rapports belges au congrès international de droit comparé*, juillet 2002, Brisbane, Bruylant, pp. 815 et s.
31. La notion d'équipement terminal est définie par la directive 99/5/CE sur l'équipement terminal de radio ou de télécommunications comme: «*a product enabling communication or a relevant component thereof, which is intented to be connected directly or indirectly by any means whatsoever to interfaces of public telecommunications networks*».
32. Certains tickets de caisse émis par des entreprises de grande distribution font ainsi apparaître le numéro de la carte qui a servi au paiement électronique des marchandises. Il est à noter que l'utilisation de ce numéro de carte permettrait de reconnaître les différents achats étalés dans le temps, effectués à l'aide de la même carte.

nécessaire pour l'accomplissement des finalités poursuivies par le commerçant dans sa relation avec le porteur de la carte.

Section 3

Banksys et la collaboration avec les autorités publiques

22. *Deux fondements légaux* – La loi du 11 janvier 1993[33] relative à la prévention de l'utilisation du système financier aux fins de blanchiment de capitaux avait déjà prescrit quelques devoirs de collaboration à charge des établissements financiers et de leurs mandataires vis-à-vis des autorités policières et judiciaires.

La loi du 28 novembre 2000 relative à la criminalité informatique[34] a étendu de manière considérable ces devoirs de collaboration qu'un prestataire de services comme Banksys doit honorer vis-à-vis des autorités policières et judiciaires.

Ces deux législations seront successivement analysées.

SOUS-SECTION 1. LA LOI DU 11 JANVIER 1993 SUR LE BLANCHIMENT D'ARGENT

23. *Banksys soumis à la loi?* – Cette loi qui a subi depuis sa promulgation diverses extensions de son champ d'application tant *ratione materiae*[35] que *personae*[36]; est-elle applicable à Banksys?

L'article 2 de la loi du 11 janvier 1993 vise en son 2° les établissements de crédit. La notion englobe, selon la loi du 22 mars 1993, les entreprises qui reçoivent du public des dépôts d'argent ou d'autres fonds remboursables et les entreprises dites «établissements de monnaie électronique» qui émettent des instruments de paiement sous la forme de monnaie électronique. L'article 2 vise également les personnes physiques ou morales qui émettent ou gèrent des cartes de crédit (13°).

Il est clair que Banksys gère, pour le compte de leurs organes émetteurs, des cartes de crédit classiques (celles Visa ou Master Card).[37] La notion de «gestion» des cartes n'est pas définie et on pourrait aussi bien considérer que Banksys est directement tenu par la loi sur le blanchiment ou n'est pas tenu par cette loi que comme mandataire des banques dont elles gèrent les cartes de paiement ou les instruments de monnaie électronique (PROTON)? La question mérite d'être posée. Par ailleurs, on note que la loi de 1993 est ambiguë. Le fait que Banksys pourrait au titre d'une de ses activités rentrer dans le champ d'application de la loi, conduit-il à lui voir appliquer la loi pour l'ensemble de ses activités?

33. *M.B.*, 9 février 1993.
34. *M.B.*, 3 février 2001.
35. En particulier, la loi du 12 janvier 2004 (*M.B.*, 23. janvier 2004) prescrit que l'obligation de collaboration mise à charge des personnes visées par le texte vise (art. 3) non seulement le terrorisme mais au-delà son financement, le commerce ou l'utilisation de substances illicites liées au bétail, le détournement par des personnes exerçant une fonction publique, à l'escroquerie, à l'abus de confiance, à l'abus de biens sociaux,...
36. La même loi de 2004 a étendu aux intermédiaires d'assurance, aux agents immobiliers et dans une certaine mesure aux avocats l'application de la loi. Sur cette dernière extension controversée, G.A. DAL et J. STEVENS, 'Les avocats et la prévention du blanchiment de capitaux: une dangereuse dérive', *J.T.*, 2004, pp. 485 et s.
37. Les cartes «carburant» ne peuvent-elles pas également être traitées de cartes de crédit?

24. *Une application malaisée de la loi* – L'application de la loi du 11 janvier 1993 conduit à des obligations[38] dont certaines pourraient heurter des principes déjà affirmés sur base de la loi de 1992 (*supra*, Section 2). L'article 4 introduit par la loi du 12 janvier 2004 oblige «les personnes visées à identifier leurs clients au moyen d'un document probant dont il est pris copie, sur support papier ou électronique». Le § 2 du même article prescrit le devoir de «vigilance constante à l'égard de la relation d'affaires» ce qui implique «un examen attentif des opérations effectuées afin de s'assurer que celles-ci sont cohérentes avec la connaissance qu'ils ont de leur client, de ses activités commerciales, de son profil de risque et lorsque cela est nécessaire de l'origine des fonds».[39]

Comment Banksys pourrait-elle satisfaire à de telles obligations? L'identité de la personne ne lui est connue que de manière ponctuelle et la vérification de celle-ci opérée par l'émetteur de la carte de paiement ou de crédit.

Par ailleurs, une telle connaissance de l'identité, nous l'avons dit, serait contraire aux principes de la loi vie privée. Pire encore, le profilage des opérations de l'individu identifié ou identifiable est un traitement incompatible avec les finalités de la collecte, selon les principes de la même loi.

La connaissance voire le soupçon d'une des infractions listées par l'article 3 de la loi du 11 janvier 1993 entraîne l'obligation de prévenir la cellule de traitement des informations financières conformément aux articles 12, 13 et 14. A nouveau, on s'interroge comment les données de trafic et de localisation rassemblées par Banksys pourraient-elles constituer pour cette dernière un indice des infractions commises par un porteur de carte, que Banksys ne connaît qu'à travers un numéro de carte.

25. *Conclusions* – L'application de la loi sur le blanchiment des capitaux à Banksys soulève de nombreuses difficultés. On peut parfaitement imaginer que les banques, les organismes émetteurs de cartes de crédit puissent à l'occasion des données de trafic ou de localisation qui lui fournit Banksys être alertés sur un déplacement suspect ou une opération étrange par rapport au comportement d'un de leurs clients. Que dans ce cas, elles-mêmes avertissent la cellule et demandent à Banksys de collaborer à la fourniture des preuves des indices à recueillir est évident. Cette assertion est cependant différente de celle qui placerait directement Banksys dans le champ d'application de la loi. Banksys serait alors mandaté par les organismes pour lesquels elle travaille de fournir aux autorités légalement désignées les renseignements relatifs à tel ou tel porteur de moyens de paiement ou de crédit. Dans une telle hypothèse, Banksys n'a point de pouvoir d'initiative mais agit strictement et pour les cas dûment spécifiés à la demande de ses «clients».

38. On note ainsi, l'obligation de sensibiliser le personnel, celle de nommer un responsable de l'application de la loi.
39. Voir également, l'article 8 qui prescrit un devoir d'attention particulière vis-à-vis de certaines opérations à considérer comme suspectes.

SOUS-SECTION 2. LA LOI DU 28 NOVEMBRE 2000 RELATIVE À LA CRIMINALITÉ INFORMATIQUE

26. *De l'obligation de collaboration* – Nous avons démontré ailleurs[40] combien l'opacité des systèmes d'information justifiait les devoirs de collaboration nouveaux consacrés par la loi. Que les experts en système d'information, les responsables et employés des entreprises qui offrent des services permettant de sécuriser ou gérer des systèmes d'information, soient appelés à aider les autorités policières à pénétrer les arcanes des systèmes et à y lire voire déchiffrer les informations y déposées, relève de l'idée que sans cette collaboration la lutte serait inégale et les systèmes d'information, accusés d'être les instruments faciles des pires crimes.

Que Banksys constitue une cible privilégiée de ces demandes de collaboration est évident.[41] Le réseau Banksys conserve, ne serait-ce que de manière éphémère, les traces des opérations cartes de paiement voire de crédit, d'une grande majorité de la population belge. Ces traces, nous localisent et renseignent sur nos opérations et habitudes de consommation. Chaque jour, les médias évoquent ainsi la découverte de délinquants permise par un tel traçage.

Le cadre légal de la collaboration entre Banksys et les autorités en charge des investigations policières est fixé par la loi citée, en particulier par les dispositions introduites dans le Code d'instruction criminelle.

27. *La collaboration lors de saisie ou de perquisition* – L'article 88*quater* est une de ces dispositions. Il autorise[42] le juge d'instruction ou un officier de police judiciaire auxiliaire du procureur du Roi «*d'ordonner aux personnes dont il présume qu'elles ont une connaissance particulière du système informatique qui fait l'objet de la recherche ou des services qui permettent de protéger ou de crypter des données qui sont stockées, traitées ou transmises par un système informatique, de fournir des informations qui, sur le fonctionnement de ce système et sur la manière d'y accéder ou d'accéder aux données qui sont stockées, traitées ou transmises par un tel système, dans une forme compréhensible*». Ainsi, la suspicion de fraude à la TVA d'un commerçant pourrait amener à une perquisition des autorités du système d'information de celui-là et la demande de collaboration de Banksys pour donner à ces autorités les renseignements nécessaires permettant l'identification des personnes ayant effectué des opérations à partir des terminaux installés dans l'entreprise. Un autre exemple: le fait que Banksys installe indépendamment des services de réseau des lecteurs de cartes et des terminaux pourrait amener des demandes relatives aux logiciels de cryptage utilisés par ces terminaux et d'aide au décryptage des messages transmis.

40. Y. POULLET, 'A propos du projet de loi dit n° 214: la lutte contre la criminalité dans le cyberespace à l'épreuve du principe de régularité des preuves', in *Liber Amicorum J. du Jardin*, Bruxelles, Kluwer, 2001, p. 5.
41. A noter ce conseil historique et «plein d'humour» donné par le FBI vers 1980 au KGB que l'on peut résumer comme suit: «Si vous souhaitez contrôler les activités de chaque citoyen de l'URSS, supprimez l'argent liquide et donnez à chaque citoyen, une carte de paiement électronique».
42. Moyennant justification de la mesure par une ordonnance motivée.

La collaboration suite à une telle ordonnance est due sous peine de sanctions pénales. Elle entraîne l'application du secret professionnel vis-à-vis des informations découvertes lors de cette collaboration.

28. *L'extension d'une perquisition au système d'information de Banksys* – L'article 88*ter* prévoit en cas de perquisition dans un système informatique, la possibilité d'extension de la recherche vers d'autres systèmes informatiques. Pour Banksys, très concrètement se pose la question de savoir si à l'occasion d'une perquisition chez un commerçant, le juge d'instruction peut aux conditions fixées par le § 1, étendre la recherche aux données tenues par Banksys? Le § 2 prévoit que l'extension de la recherche ne peut excéder les parties du système informatique auxquelles «*les personnes autorisées à utiliser le système informatique ont spécifiquement accès*». Ces limites reçoivent une extension différente suivant les cas: ainsi, dans le cadre d'un P.O.S., on peut imaginer que seules les données toujours présentes dans le terminal installé chez le commerçant et qui sont envoyées en batch pourraient faire l'objet d'une demande d'extension d'accès dans la mesure où l'accès à l'ensemble des autres parties du système Banksys n'est pas autorisé aux commerçants. Dans le cadre de cartes de fidélité, on pourrait concevoir que les bases de données recensant les opérations faites à partir de ces cartes présentes dans le système informatique de Banksys soient accessibles dans le cadre d'une extension de perquisition ordonnée par les autorités judiciaires dans la mesure où ces bases de données seraient facilement accessibles à l'émetteur des cartes lui-même.

29. *L'aide au repérage et à l'écoute* – L'article 88*bis*, § 1er permettait déjà dès 1998[43] au juge d'instruction de procéder à un repérage des télécommunications et «d'obtenir pour ce faire le concours technique de l'opérateur d'un réseau ou le fournisseur d'un service de télécommunications». Il s'agissait de permettre le repérage tant des données d'appel de moyens de télécommunications à partir desquels ou vers lesquels des appels sont adressés et la localisation de l'origine et de la destination. L'ordonnance du juge est motivée et communiquée au Procureur du Roi.

A ces mesures de repérage, l'article 90*ter* ajoute des mesures permettant l'écoute en temps réel des communications lorsque les nécessités de l'instruction l'exigent..., «s'il existe des indices sérieux que le fait dont il est saisi constitue une infraction visée par l'une des dispositions énumérées par le § 2[44], et si les autres moyens d'investigation ne suffisent pas à la manifestation de la vérité».[45] Cette écoute s'opère vis-à-vis de personnes soupçonnées sur base d'indices précis ou à l'égard de moyens de communications régulièrement utilisés par un suspect, ou à

43. Loi du 10 juin 1998.
44. La liste reprise à l'art. 90*ter*, § 2 et étendue à de multiples reprises se réfère à plus de 20 infractions considérées comme graves.
45. Sur ces conditions et leur interprétation, lire J. DUMORTIER, J. VAN OUDENHOVE et P. VAN EECKE, «La nouvelle législation belge relative à la criminalité informatique», *Vigiles*, 2001, pp. 44-62; C. MEUNIER, «La loi du 28 novembre 2000 relative à la criminalité», in *Actualités du droit des technologies de l'information et de la communication*, CUP, vol. 45, fév. 2001, pp. 95-148.

propos de lieux présumés fréquentés. Ainsi, le juge[46] pourrait mettre sur «écoute» le terminal d'un commerçant suspecté d'escroquerie ou surveiller le fonctionnement de différents terminaux de télépéage pour connaître les personnes empruntant à un certain moment, les autoroutes situées près du lieu d'un crime.

30. *Le stockage des données «d'identification»* – Par l'insertion d'un article 109*ter* E, § 2 dans la la loi du 21 mars 1991[47], la loi de 2000 ajoute, à ces divers devoirs de collaboration, une obligation qui vise l'ensemble des opérateurs de réseaux et des fournisseurs de services d'enregistrer et de conserver, pendant un délai minimal de 12 mois «*en vue de l'investigation et de la poursuite d'infractions pénales, les données d'appel de moyens de télécommunications et les données d'identification d'utilisateurs de services de télécommunications*».[48] Cette obligation concerne à l'évidence Banksys à la fois opérateur de réseaux et en outre souvent fournisseur de services de télécommunication.

L'arrêté royal du 9 janvier 2003 portant exécution des articles 88*bis*, 90*quater* du Code d'instruction criminelle, de même que de l'article 109*ter* E, § 2 de la loi du 21 mars 1991 précise les données à conserver par les différentes catégories visées, en particulier pour les fournisseurs de services de télécommunications qui utilisent différentes technologies, comme c'est le cas de Banksys (paiement via Internet, paiement via les mobiles et via des terminaux fixes). L'article 7, 5° considère qu'ils «*doivent donner toutes les données d'appel (numéro de l'appareil terminal sortant, date de la communication, heure de début, durée de la communication) et de localisation relative aux différentes phases et aux services utilisés de la télécommunication telles qu'elles sont imposées aux diverses catégories d'opérateurs et de fournisseurs de services*». Il s'agit en effet par l'intégration de l'ensemble des données relatives à l'utilisation des divers réseaux empruntés (p. ex. les réseaux mobilophones et en cas d'un paiement à partir du mobile et fixe la connexion internet avec l'ISP et le réseau fixe en cas d'un paiement via Internet) de pouvoir reconstituer l'ensemble de la relation entre l'origine de la communication et sa destination.

31. *Les obligations liées aux devoirs de collaboration de Banksys comme opérateur de réseaux et fournisseurs de services* – L'arrêté royal cité ci-dessus oblige les entreprises visées à désigner «nommément une ou plusieurs personnes chargées d'assumer les tâches résultant de l'obligation de coopérer et dénommée(s) la *cellule de coordination de la justice*». Les noms sont transmis à l'Institut belge de services postaux et de télécommunications et par l'Institut aux autorités judiciaires compétentes. La communication de données que cette cellule devra transmettre aux autorités judiciaires se fera suivant certains standards y compris

46. ... ou le procureur du Roi en cas de flagrant délit (art. 90*ter*, § 5).
47. Il s'agit de la loi portant réforme de certaines entreprises publiques économiques, loi dite «Belgacom».
48. Sur cette obligation, lire notre article, «The Fight against Crime and/or the Protection of Privacy; A Thorny Debate», 18 *Int. Rev. of Law Computers & Technology*, 2004, n° 2, pp. 251-273. A noter également l'avis de la Commission de protection de la vie privée, avis n° 33/99 du 13 décembre 1999 relatif à l'avant-projet de loi sur la criminalité informatique, avis disponible sur le site de la Commission (*http://privacy.fgov.be*).

techniques et répondra à des exigences fonctionnelles comme fixé aux articles 6 et 8. On notera que les frais d'investissement, d'exploitation et d'entretien des systèmes permettant aux opérateurs et fournisseurs de répondre aux demandes sont à charge de ces derniers. Par contre, les frais de collaboration sont remboursés selon des tarifs précisés en annexe.

Section 4

Conclusions

32. *Plus de questions que de réponses* – Au terme de ce tour d'horizon des questions de vie privée nées de l'analyse du fonctionnement des services et produits de Banksys, l'auteur est bien tenu de reconnaître son double embarras. Premièrement, l'application des lois est incertaine: la loi du 8 décembre 1992, pilier de la protection des données demain. Une première raison touche certainement à résoudre pour assurer la protection des données à caractère personnel est-elle applicable à Banksys en tant que sous-traitant ou de responsable du traitement? Les conséquences de la réponse à cette question sont lourdes. La directive 2002/58 et sa prochaine transposition en droit belge définissent un champ d'application qui, confronté à la réalité des services offerts par Banksys, s'avère difficile à tracer. Les mêmes incertitudes existent à propos de la loi sur le blanchiment d'argent dont l'application à Banksys exigerait un approfondissement de la nature et des conséquences du mandat qui serait confié à Banksys. Sans doute, les réponses à peine ébauchées présentées ici méritent-elles d'être approfondies avec une pleine connaissance tant de la réalité du terrain qu'un travail avec les autorités en charge de l'application de lois nouvelles souvent rédigées à la hâte et sans souci de cohérence entre elles.[49]

33. *Des questions essentielles cependant pour l'avenir de la protection des données* – L'analyse du fonctionnement de Banksys révèle des questions qui, on le pressent, seront essentielles à résoudre pour assurer la protection des données demain. Une première raison touche certainement aux services offerts: Banksys offre un service dont l'utilité devient chaque jour plus criante, le service de paiement électronique via des cartes de paiement ou de crédit. La quasi totalité de la population belge utilise de tels services et ce, de plus en plus fréquemment. Les traces laissées par l'utilisation des services de Banksys permettent un profilage de personnes dont l'intérêt n'échappe ni à des entreprises privées soucieuses de leur marketing, ni aux pouvoirs publics, soucieux de la sécurité publique. Banksys se doit de répondre à ces appétits à la fois par une parfaite sécurité de ses réseaux et de ses produits et par un souci constant de respecter les principes mêmes de la loi de protection des données et les limites des investigations de l'autorité.

Une seconde raison touche aux technologies utilisées: celles relatives à la communication où les services de Banksys empruntent et intègrent pour offrir ces services les divers réseaux: mobiles, câbles, etc.; les paiements par Internet se généralisent. Quant au support proposé, le débat sur la carte multifonctionnelle semble inévitable. Banksys sera inévitablement confronté à des questions nou-

49. A cet égard, nous avons souligné l'utilisation par la directive 2002/58/CE de concepts différents de ceux de la directive 1995/47/CE, dont elle n'est pourtant, selon ses auteurs, qu'une application sectorielle.

velles. Comment assurer la sécurité et la confidentialité des transmissions lors de l'utilisation des cartes de paiement et de crédit sur Internet? Comment développer des lecteurs de cartes multifonctionnelles répondant aux exigences de la protection des données et assurant que les applications logées par Banksys seront opérées en toute sécurité?

Bref, l'étude ne fait que commencer. Il me reste à remercier les organisateurs de cet événement de m'avoir permis d'en poser les premiers jalons.